PUBLIC KEY INFRASTRUCTURE IMPLEMENTATION PLAN

The Marine Corps has been a leader in DoD's implementation and management of Public Key Infrastructure (PKI) and the issuing of Common Access Cards (CAC). Since the activation of DoD PKI in May 1999, the Marine Corps has aggressively installed PKI to DoD standard across the Marine Corps Enterprise Network (MCEN).

In November of 1999, DoD mandated that the CAC would become the token utilized for both physical access to buildings as well as logical access to networks. Since 2001, the Marine Corps successfully installed a CAC infrastructure and issued nearly two million cards. Nearly 80% of all Marines currently hold a CAC.

Last year several other milestones were achieved. The Marine Corps Network Operations Center implemented the initial repository for public key encryption certificates. Device and software certificate issuance exceeded 600 and 30,000 respectively. The Marine Corps completed procurement of over 80,000 CAC readers and middleware for use during the transition from software certificates to CAC use at individual workstations. Finally, the Marine Corps proved its ability to issue PKI certificates in operational environments such a Afghanistan and Iraq.

The Marine Corps now must implement two necessary infrastructure upgrades: a series of directories and Online Certificate Status Protocol (OCSP) responders. These components will allow the Marine Corps to meet DoD requirements for implementing cryptographic logon with the CAC, as well as providing the user a method of validating digitally signed emails and documents.

The Marine Corps remains firmly committed to the implementation of PKI and the enabling of applications to take advantage of the security services that PKI provide. We continue to support DoD PKI requirements for specific programs and mission needs as they arise and are engaged in the development of procedures and policies for the implementation of PKI on the SIPRNET.